EXHIBIT E

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2012 Issue


Brian R. Strange


David A. Holop


Jennifer Lin

Privacy: Is it legal "tracking" or an illegal wiretap?

Sorting out whether the federal Wiretap Act applies can be a highly technical endeavor

Online and mobile communication technology is an everyday part of the lives of most Americans today: a 2010 survey by the Pew Internet and American Life Project found that 82 percent of Americans use cell phones, and a study by the World Bank similarly estimated that almost 80 percent of Americans use the Internet. These numbers will only continue to grow in the years to come as technology becomes even cheaper and more available. While these technologies bring many benefits to users, the rise in the prevalence of online and mobile technology also brings with it increasing concerns about the privacy of users and their data. It seems every month a new privacy issue arises as technology companies push the limits of data tracking and collection, and each new issue brings along with it a myriad of important legal privacy issues. For example, when can a cell phone company legally track the physical movements of its users, or to what degree can an Internet company monitor the online activities of its users? These questions and many more like it contribute to a burgeoning area of the law that lawmakers have struggled to keep up with, leaving consumers to seek remedies under existing laws written for older technologies.

These privacy issues have become much more salient in recent years, as media reports of "tracking" have became more frequent. An example of a controversial practice was brought to light in 2010, when it was revealed that Apple had been collecting and storing users' geographical locations in their iPhones and iPads. This created a large security issue because this user information was available to anyone who had remote access to the user's iPhone or iPad. A number of class-action lawsuits were filed against Apple and other mobile service providers, and the litigation is still playing out in federal court. (*In re iPhone Application Litig* (N.D. Cal. 2011) No. 11-MD-02250-LHK.) Another example came to light in late 2011, when reports surfaced that a tracking software called Carrier IQ was embedded in millions of cell phones. Litigation is now proceeding against the maker of the software and phone manufacturers. (*In re Carrier IQ, Inc., Consumer Privacy Litig.* (N.D. Cal. 2012) MDL No. 2330.)

Apart from users' physical locations, tech giants such as Google and Facebook, as well as many smaller Internet companies and start-ups, are interested in collecting much more data on users' online activities: their demographic information, their interests, whom they communicate with, and so on – anything you can imagine. This, too, while not necessarily a new practice (*e.g.,* tracking cookies have been around for many years) has been the subject of recent controversy. For example, earlier this year, a privacy researcher found that Google (and three other online advertising companies) circumvented browser settings that were in place to block tracking by third-party cookies. Apple's Safari browser was designed to prevent third-party cookies by default, but according to the researcher, Google and the other advertising companies made it possible for the cookies to still load and track users' Web browsing activities. In a similar vein, Facebook also faced a class-action lawsuit over allegations that it transmitted user information to third-party advertisers without the users' consent. (*In re Facebook Privacy Litig.* (N.D. Cal. 2010) No. C 10-02389 JW.)

With all these privacy threats, consumers continue to look to the courts to seek remedy when their personal privacy has been breached online. One source of relief available to wronged consumers under federal law is the Electronic Communications Protection Act of 1986 ("ECPA"), which includes the Wiretap Act and the Stored Communications Act ("SCA"). While these laws have not always kept up with the pace of technology, they still provide the opportunity for consumers to find relief when their privacy has been violated.

The Wiretap Act

The ECPA is the main source of regulation of providers of wireless or electronic communications services. Title I of the ECPA is the Federal Wiretap Act, and Title II of the ECPA is the SCA. Both statutes establish privacy protections for consumers against the government and private parties. Consumers who are interested in protecting the privacy of their communications are likely just as worried about online or mobile companies turning over user data to the government as they are about this information getting into the hands of third parties, such as advertisers. The Wiretap Act focuses on the *interception* of consumers' electronic or wireless communications, while the SCA covers retrieval of that information from *storage* without the consumers' consent.

The Wiretap Act gives consumers a private right of action against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." (18 U.S.C. § 2511(1)(a).) At its core, all that is required is that a communication is intercepted. The law does not require that the interceptor improperly use the communication, share it or do anything else with it. It is important, however, to understand how courts have parsed the language of the law to limit its reach.

See Strange, Holop & Lin, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2012 Issue

Courts have generally interpreted "interception" as referring only to communications that were acquired while in transit, not those acquired while in storage. (See *Konop v. Hawaiian Airlines, Inc.* (9th Cir. 2002) 302 F.3d 868, 878 [an interception can occur only while the electronic message is being transmitted]; *Fraser v. Nationwide Mut. Ins. Co.* (E.D. Pa. 2001) 135 F. Supp. 2d 623, 635 [retrieval of e-mail message from intermediate or back-up storage while message is in the course of transmission is "interception" under Federal Wiretap Act; retrieval of message from post-transmission storage is not]; and *U.S. v. Steiger* (11th Cir. 2003) 318 F.3d 1039, 1049 [e-mail can only be intercepted during "flight"].) Other courts, however, have allowed for a broader reading of the term "interception," holding it includes the acquisition of messages that "reside briefly in the memory of" devices transmitting the messages. (See, *e.g.*, *United States v. Szymuszkiewicz*, (7th Cir. 2010) 622 F.3d 701, 706.) Thus, for a consumer to have a viable claim under the Wiretap Act, he or she may have to show that the electronic or wireless services provider intercepted (or tried to intercept) his or her communication while it was in transit. Proving this can become quite technical and fact-dependent, and may limit the law's application.

In addition, while plaintiffs do not have to show that the interceptor took any bad actions with regard to the information, they may have to show that the defendant electronic or wireless services provider had access to the *contents* of the communication. Courts have held that "transactional information" about the communication – the fact that it was made and between whom – is not enough to give rise to an "interception." (*U.S. v. Lazu-Rivera* (D.P.R. 2005) 363 F. Supp. 2d 30, 38.) For example, "recorded phone numbers in a cell phone's memory are not the contents of a communication," but conversations or text messages are such "contents." (*U.S. v. Parada* (D. Kan. 2003) 289 F. Supp. 2d 1291, 1304.) This requirement presents a potential hurdle to consumers whose claims arise from the electronic service providers' disclosure to third-party advertisers that they visited a particular Web site at a particular time or the fact that they interacted with a third-party via text message or e-mail – this information may be construed as being merely "transactional," though the case law on this issue is still being developed. Where the tracking party actually did intercept the "contents" of online or mobile communications or activity, plaintiffs would more likely be successful in such actions.

Further, the Wiretap Act also provides that defendants accused of interception are protected from liability when one of the parties to the communication has given prior *consent* to the interception. (18 U.S.C. § 2511(2)(c-d).) As an example, courts have found consent when plaintiffs continued using an Internet service provider's ("ISP") services after being informed in the user agreement of the possibility that data regarding their usage would be shared with unnamed third parties. (*Kirch v. Embarq Management Co.* (D. Kan. Aug 19, 2011) 2011 WL 3651359, at *7-9.) Courts have stated that "Congress intended the consent requirement to be construed broadly," but "consent should not casually be inferred." (*Griggs-Ryan v. Smith* (1st Cir. 1990) 904 F.2d 112, 116-17.) Thus, consumers who have given consent in any agreed-to terms of service, or even implied consent, may be barred from bringing these claims as well, but it must be actual rather than constructive consent. (See *United States v. Footman* (1st Cir. 2000) 215 F.3d 145, 155.) Where there is insufficient evidence of consent, the defense will not apply. (See, *e.g.*, *In re Pharmatrak, Inc.* (1st Cir. 2003) 329 F.3d 9, 20.) While some actions by consumers may indicate consent, when a tracking company exceeds any terms of service or covertly tracks without any action by the user that would indicate consent, consent should not be found to bar a Wiretap Act claim.

Another option for a plaintiff who seeks relief under the Wiretap Act lies in its provision that prohibits electronic communication service providers from knowingly divulging the contents of any communication while it is in transmission to anyone but the person or entity who is the intended recipient of that communication. (18 U.S.C. § 2511(3)(a).) There is an exception for situations in which the recipient consents to the divulgence. (18 U.S.C. § 2511(3)(b)(ii).) The plaintiffs in *In re Facebook Privacy Litigation* attempted to base their Wiretap Act claim on this premise. The court found that the plaintiffs had alleged facts sufficient to establish that they had suffered the injury required for standing under Article III of the U.S. Constitution on this claim, but nevertheless dismissed the claim based on the particular facts at issue.

The court found that the consumer, when he or she clicked on a third-party advertising banner on Facebook, was essentially sending a communication to either the advertiser or Facebook. There were two interpretations of this "communication" of clicking the ad under the Wiretap Act: either Facebook was the intended recipient and was therefore immune from liability, or, if the third-party advertiser was considered the recipient, Facebook could not be held liable for divulging plaintiffs' information to that intended recipient. ((N.D. Cal. 2011) 791 F. Supp. 2d 705, 712-13.) Again however, under different circumstances where the user has not taken an action like clicking on an advertisement (*e.g.*, if the user is sending a message to a contact), the Web site or third party would not be the intended recipient of that type of communication.

There have been a number of cases where plaintiffs have been able to make cognizable Wiretap Act claims based on the invasion of their privacy and unauthorized use of their personal data. For example, in *U.S. v. Councilman* (1st Cir. 2005) 418 F.3d 67, 80, the First Circuit held that providers of an online rare books listing service which gave its subscribers e-mail addresses and then stored copies of all incoming e-mails from Amazon.com, a competitor, could be liable under the Wiretap Act. Likewise, the court in *Elk Grove Answering Service v. Hoggatt* (E.D. Cal. Nov. 15, 2010) 2010 WL 4723720, at *2, held that the plaintiff, who worked at a

See Strange, Holop & Lin, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2012 Issue

telephone company and alleged that her co-workers accessed the company's server to download her personal calls to third parties, had sufficiently pled a Wiretap Act claim. These courts' interpretations of the Wiretap Act show that claims can go forward under the right set of facts.

While there are some barriers to claims under the Wiretap Act, plaintiffs can succeed if they properly allege facts showing an interception of the contents of their communications without consent. If a plaintiff is able to prevail on a Wiretap Act claim, he or she may be entitled to equitable or declaratory relief, damages including potentially punitive damages in appropriate cases, as well as attorney's fees and litigation costs. (18 U.S.C. § 2520(b).) A court computing damages may assess the greater of the sum of the plaintiff's actual damages and any profits made by the defendants, or statutory damages of "the greater of $100 a day for each day of the violation or $10,000." (18 U.S.C. § 2520(c)(2).) These may be substantial damages in a case of widespread tracking.

Stored Communications Act

The other important title under the ECPA for consumers whose privacy has been breached online is the Stored Communications Act. The SCA states that an electronic communication service ("ECS") provider "shall not knowingly divulge to any person or entity the contents of a communication while in electronic *storage* by that service." (18 U.S.C. § 2702(a)(1) (emphasis added).) The SCA also prohibits remote computing service ("RCS") providers from knowingly divulging to any person or entity "the contents of any communication that are carried or maintained on that service...on behalf of...a subscriber or customer of such service." (18 U.S.C. § 2702(a)(2).)

Similar to claims under the Wiretap Act, a plaintiff who prevails on an SCA claim may be entitled to equitable or declaratory relief, damages, attorney's fees and litigation costs. (18 U.S.C. § 2707(b).) More specifically, in calculating damages, the court should assess the sum of actual damages that the plaintiff suffered and any profits that defendants made as a result of the violation. The statute states that a plaintiff shall, in no case, be entitled to less than $1,000, and punitive damages may be available if the violation is willful or intentional. (18 U.S.C. § 2707(c).) In order to bring an SCA claim, a plaintiff need not have a contractual agreement with the ECS or RCS provider. (See *Quon v. Arch Wireless Operating Co*. (C.D. Cal. 2004) 309 F. Supp. 2d 1204, 1209.)

Whether an entity is defined as an ECS or an RCS has consequences for its right to disclose information. The difference between an ECS and RCS is that an ECS provides a service that enables users to send or receive wire or electronic communications. (18 U.S.C. § 2510(15).) An RCS, on the other hand, provides only computer storage and processing services. (18 U.S.C. § 2711(2).) While RCSs are permitted to release the contents of a communication with the lawful consent of a *subscriber*, an ECS may release the contents of a communication only with the lawful consent of the *originator* of the message or one of its intended *recipients*. (18 U.S.C. § 2702(b)(3) (emphasis added).)

Courts have held that the SCA applies to telephone companies, Internet or e-mail-service providers, and bulletin board services. (*Becker v. Toca* (E.D. La. Sept. 26, 2008) 2008 WL 4443050, at *4.) Courts have also held that ISPs that store e-mails on their servers for back-up protection are ECSs. (*Theofel v. Farey-Jones* (9th Cir. 2004) 359 F.3d 1066, 1070.) Social networking sites that provide private messaging and e-mail services have also been found to be ECSs under the SCA. (*Crispin v. Christian Audigier, Inc.* (C.D. Cal. 2010) 717 F. Supp. 2d 965, 982.) An example of an RCS would be the operator of a "computer bulletin board." (*Steve Jackson Games, Inc. v. U.S. Secret Service* (W.D. Tex. 1993) 816 F. Supp. 432, 443.) Also, when entities such as You Tube store videos that users mark as "private," they are acting as "storage entities" and are considered RCSs. (*Crispin*, 717 F. Supp. 2d at 990.) Sorting out whether a technology is an ECS or an RCS can be a highly technical endeavor, but an important one for applying the provisions of the SCA and determining whether plaintiffs will have a remedy under the law.

In *In re Jetblue Airways Corp. Privacy Litig.* (E.D.N.Y. 2005) 379 F. Supp. 2d 299, 307), the district court held that an airline company that operates a Web site that receives and transmits data from and to its customers "is not [a] provider of [an] electronic communication service" within the meaning of the ECPA. The airline is better characterized as a "provider of airline services" and a "consumer of electronic communication" rather than an ECS provider. Its Web site is analogous to a telephone that enables the airline to communicate with its customers. Just as mere operation of the telephone would not transform the company into a telephone services provider, operation of the Web site does not transform the company into an ECS provider within the meaning of the SCA. At the same time, Web sites certainly *can* be ECSs. In *Kaufman v. Nest Seekers, LLC* (S.D.N.Y. Sept. 26, 2006) 2006 WL 2807177, at *6, a different federal district court held that "[a]n on-line business which provides its customers, as part of its commercial offerings, the means by which the customers may engage in private electronic communications with third-parties may constitute a facility through which electronic communication service is provided." Therefore, if a Web site or other online business, such as the provider of a messaging or social networking application, provides the means of sending "electronic communications," the company may be found to be an ECS.

Similar to the Wiretap Act, the SCA's reach is limited by the consent defense. The SCA provides that liability can be excused "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." (18 U.S.C. § 2702(b)(3).) However, as under the Wiretap Act, to the extent the information is obtained without any consent by the user, plaintiffs will be able to bring their claims under the SCA.

See Strange, Holop & Lin, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2012 Issue

Settlements, other causes of action

While some issues exist regarding modern claims under the ECPA, recently plaintiffs have successfully settled a number of cases involving Wiretap Act and SCA claims. For example, in 2011, Google agreed to an $8.5 million settlement relating to the launch of its Google Buzz service, which revealed information about the names of users' e-mail contacts if users activated Buzz without changing the defaults. The parties also reached settlements in lawsuits stemming from the alleged use of Flash cookies by online marketing firms Quantcast, Clearspring, Specific Media, and Say Media's VideoEgg, which tracked users' online activities. Facebook similarly settled a suit over its Beacon program which tracked user activity and shared it with third parties. These settlements show that consumers can reach favorable resolutions on these types of tracking claims.

In addition, consumers can pursue other causes of action in these tracking cases under both federal and state laws, such as the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030), state unfair competition statutes (*e.g.,* California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*), and common law claims such as trespass to chattels, or conversion. (See, *e.g., CompuServe, Inc. v. Cyber Promotions, Inc.* (S.D. Ohio 1997) 962 F. Supp. 1015, 1023.) Other statutes requiring Web site operators to post their privacy policies (see, *e.g.*, Cal. Bus. & Prof. Code § 22575) or that forbid knowingly damaging or destroying computer programs (see, *e.g.*, Cal. Pen. Code § 502(c)(4)) may also be useful to consumers. Each of these types of action will have its own issues and limitations, which are beyond the scope of this article. However, these causes of action provide additional avenues to hold electronic and wireless communications providers accountable for deceptive trade practices and give consumers additional remedies when they have been harmed by the improper tracking and disclosure of their sensitive personal information.

On the government side, two important agencies, the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC"), are responsible for protecting consumer privacy. These agencies have also been involved in actions against technology companies accused of breaching consumer privacy recently, such as in enforcement actions against Google regarding its Buzz service and actions against online advertisers, such as Chitika, which collected and sold tracking information about users.

Consumers and consumer advocates have also called on legislatures to update the laws to protect consumers further against the current threats they face. In recent years, Congress and state legislatures have introduced "Do-Not-Track" legislation, though none has been enacted into law to-date. The proposed federal law would require the FTC, which presently does not have the authority to require entities to provide an opt-out procedure, to introduce one for consumers who do not want their online activities to be tracked. Specifically, consumers who want to prohibit the collection and use of information such as the Web sites they visited, telephone numbers, and their location (GPS-type tracking) would be able to do so under this legislation. Some Internet companies, such as Yahoo and Mozilla (creator of the popular Firefox browser), have already created "Do Not Track" options for users. In addition, the FTC has recently called for legislation regulating "data brokers," companies that buy and sell personal data to help build online profiles of consumers.

New legislation and regulation may provide more protection to consumers, but they should be accompanied by updates to the ECPA or create other private rights of action that will better protect consumers against the threats they face today. For example, a bill was introduced in California in 2011 that would not only give consumers an opt-out option, but also a private right of action against businesses that violate the law. Entities that engage in tracking would have to disclose the purpose of the tracking (*i.e.*, the intended use of the information) and how they track. (S.B. 761 (Cal. 2011).) While the bill has not yet been voted on, it is a sign that legislatures are moving in the right direction. Until more protective legislation is enacted, consumers can keep fighting under the ECPA and other existing laws to seek the remedies they deserve when their rights to privacy have been breached online and on their mobile devices.

Brian R. Strange, the founding partner of Strange & Carpenter *in Los Angeles, CA, has focused his practice for over 20 years on class action and complex business litigation, with a specialty in Internet privacy and antitrust class actions. He is currently serving on the plaintiffs' steering committee in* In re Sony Gaming Networks and Customer Data Security Breach Litigation. *David A. Holop, an associate at* Strange & Carpenter, *specializes in class action and Internet privacy litigation. Jennifer Lin is a law clerk at* Strange & Carpenter.